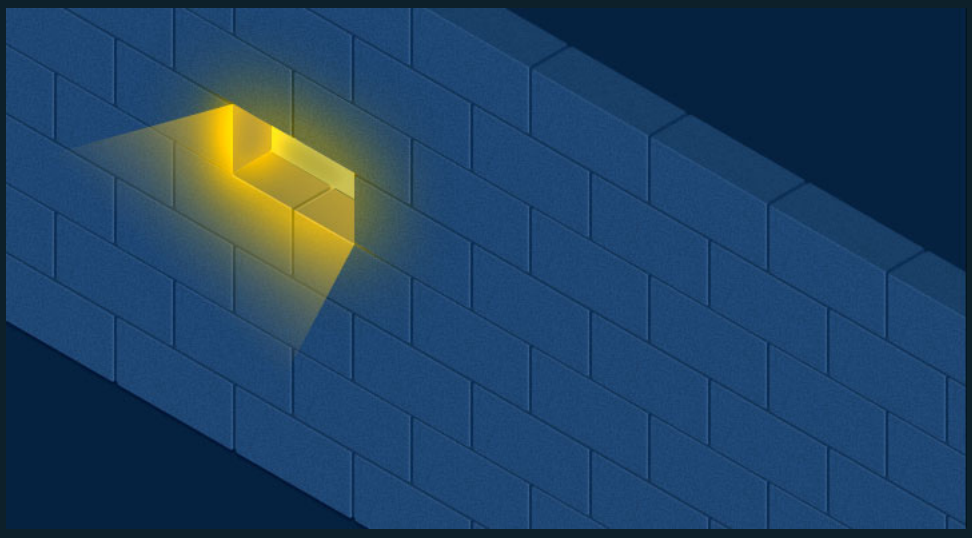
What is a Hacker (part 2): How data is stolen

The simple answer is that hackers break into computers by exploiting vulnerabilities. The vulnerability might not even be computer-related; it can be a new employee unfamiliar with the companies security routines.

Finding vulnerabilities

They exist in all systems, and there are two kinds; known and unknown.



Known vulnerabilities are often the result of needed capabilities. For example, if all users work in the same system, you have a known vulnerability; users. If that system communicates over the internet, you have another known vulnerability; remote access.

Unknown vulnerabilities are unknown to the system operator but known to the hacker. For example, large organizations use a multitude of different software, and some of these might be poorly coded, leaving vulnerabilities for a hacker to exploit.

Most hackers employ vulnerability scanners, a software that scans a network looking for

known vulnerabilities such as open ports, unpatched software, etc.

Bad passwords are a good source of access; password cracking programs can figure out poor passwords in minutes. If the hacker knows the name of the user (i.e. John Doe) he can quickly find additional information on social media that he feeds to the password cracker. The password cracker can easily identify names, dictionary words, and even common phrases.

Sometimes the simplest methods can be the most efficient ones. Hackers can gain access through unguarded computers at a receptionist's desk or in a busy office environment. Even a guarded computer can be accessed if the hacker has good social engineering skills; posing as a guy from the IT-department can be enough.

Attacking the system

Only when the hacker knows how the network infrastructure is set up, and it's vulnerabilities he initiates the attack.

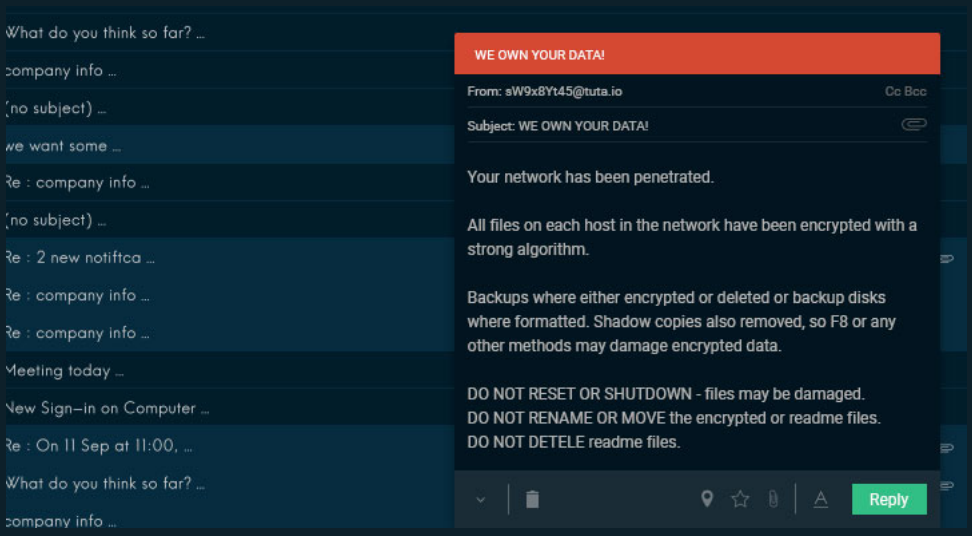
If the hacker knows the target hardware and vulnerabilities, he can tailor a specific attack for that computer or set of computers. Another approach is to target vulnerabilities without any specific target; the goal is to reach as many targets as possible. This approach eliminates the need for a specific target, but the outcome and effectiveness are less predictable.

In a tailored attack against a specific target, the hacker identifies the weakest link to attack; this might be a receptionist or other low-level employee in a large company. He might tailor an email that looks legitimate but contains either an infected PDF-file or a link to a website that is infected by the same malware. Once the receptionist opens the PDF or clicks the link their computer becomes infected, and the hacker has a way into their system.

In other more unusual attacks, hackers send a package containing office supplies to a company; a hidden bottom layer of the package contains autonomous custom hacking hardware. This method is known as "warshipping" and in essence it's a physical trojan horse; the hardware in the box breaks into the company's wifi from the inside and scans and exploits vulnerabilities. Once the custom hackerware has found and exploited a vulnerability it automatically opens up a back door for the hacker.

The aftermath

Depending on the need of the hacker, he might steal specific data, or leave malware running on the system, constantly scooping up interesting data.



If the hacker is confident his intrusion isn't going to be detected, he can leave his malware and backdoors running on the server, sometimes for years without detection. The malware might constantly scan the network for certain file types or even specific strings of text that are of interest to the hacker.

In most cases, the hacker will exploit what data he can and then cover up his tracks, deleting the malware or reverting the changes to the system so it cannot be tracked back to him. If the hack and vulnerability are purely technical and goes undetected, the same exploit can be used multiple times.

Data gathered from the attack can be used in different ways; most of the time for the monetary gain, sometimes it's for fame. The hacker might encrypt all files on the target computer, sending extortion emails to the user asking for money to provide a decryption-key.

Data can be put up for sale on darknet marketplaces, access to specific systems can be sold, database dumps of users, credit card dumps or access to botnets for DDoS attacks.

Original post can be found at our homepage:
https://www.bitidentify.com/blog/hacker-how-data-is-stolen/